

Thank you for signing in early

The webinar will begin promptly at
12:00 pm ET, 9:00 am PT



SERDP and ESTCP Webinar Series

***The webinar will begin promptly at 12:00 pm ET,
9:00 am PT***

- You have two options for accessing the webinar
 1. Listen to the broadcast audio if your computer is equipped with speakers
 2. Call into the conference line: 303-248-0285
Required conference ID: 6102000
- For any question or issues, please email serdp-estcp@noblis.org or call 571-372-6565

Cloud Computing Services for DoD: We Are Going To The Cloud!

March 22, 2018



Welcome and Introductions

Jennifer Nyman, Ph.D., P.E.
Webinar Facilitator



Webinar Agenda

- **Webinar Logistics** (5 minutes)
Dr. Jennifer Nyman, Geosyntec Consultants
- **Overview of SERDP and ESTCP** (5 minutes)
Mr. Timothy Tetreault, SERDP and ESTCP
- **Cloud Computing Services for DoD** (50 minutes)
Dr. Michael Chipley, The PMC Group
Ken Kurz, COPT
- **Q&A session** (30 minutes)

How to Ask Questions

Type and send questions at any time using the Q&A panel

Chat with Presenter:

In Case of Technical Difficulties

- Delays in the broadcast audio
 - Click the mute/connect button
 - Wait 3-5 seconds
 - Click the mute/connect button again
 - If delays continue, call into the conference line
 - Call into the conference line: 303-248-0285
 - Required conference ID: 6102000
- Submit a question using the chat box

SERDP and ESTCP Overview

Timothy Tetreault
Installation Energy and Water
Program Manager



SERDP

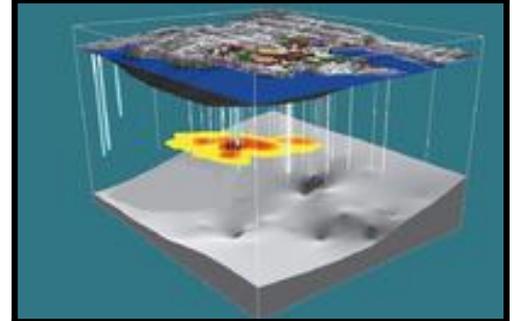
- Strategic Environmental Research and Development Program
- Established by Congress in FY 1991
 - DoD, DOE and EPA partnership
- SERDP is a requirements driven program which identifies high-priority environmental science and technology investment opportunities that address DoD requirements
 - Advanced technology development to address near term needs
 - Fundamental research to impact real world environmental management

ESTCP

- Environmental Security Technology Certification Program
- Demonstrate innovative cost-effective environmental and energy technologies
 - Capitalize on past investments
 - Transition technology out of the lab
- Promote implementation
 - Facilitate regulatory acceptance

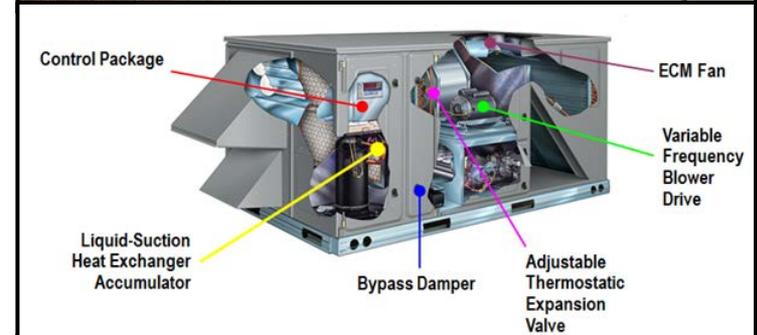
Program Areas

1. Installation Energy and Water
2. Environmental Restoration
3. Munitions Response
4. Resource Conservation and Resiliency
5. Weapons Systems and Platforms



Installation Energy and Water

- Smart and secure installation energy management
 - Microgrids
 - Energy storage
 - Ancillary service markets
- Efficient integrated buildings and components
 - Design, retrofit, operate
 - Enterprise optimized investment
 - Advanced components
 - Intelligent building management
 - Non-invasive energy audits
- Distributed generation
 - Cost effective
 - On-site
 - Emphasis on renewables



SERDP and ESTCP Webinar Series

Date	Topic
April 5, 2018	Advanced Nanocrystalline Cobalt Alloys and Composites as Alternatives for Chromium and Nickel Plating in Repair Operations
April 19, 2018	Sediment Volume Search Sonar
May 3, 2018	Overview of the Defense Coastal/Estuarine Research Program (DCERP)
May 17, 2018	Environmental Restoration Program Area Webinar
May 31, 2018	Resonant Acoustic Mixing of Energetic Material Formulations

For upcoming webinars, please visit

<http://serdp-estcp.org/Tools-and-Training/Webinar-Series>



Save the Date

SERDP • ESTCP
SYMPOSIUM
2018 | Enhancing DoD's Mission Effectiveness

A three-day symposium showcasing the latest technologies that enhance DoD's mission through improved environmental and energy performance

November 27 - 29, 2018

Washington Hilton Hotel

Registration is coming soon

Cloud Computing Services for DoD *We Are Going To The Cloud!*

Dr. Michael Chipley
The PMC Group LLC
Ken Kurz
COPT



Agenda

- Why the Cloud?
- DEPSECDEF Rapid Adoption of Cloud Memo 2018
- DoD CIO Cloud Policy
- FRCS Traditional Architecture
- FRCS Cloud Architectures
- R&D Needs
- Virtual Power Station for Naval Facilities
- COPT Leased Facilities – Private Cloud

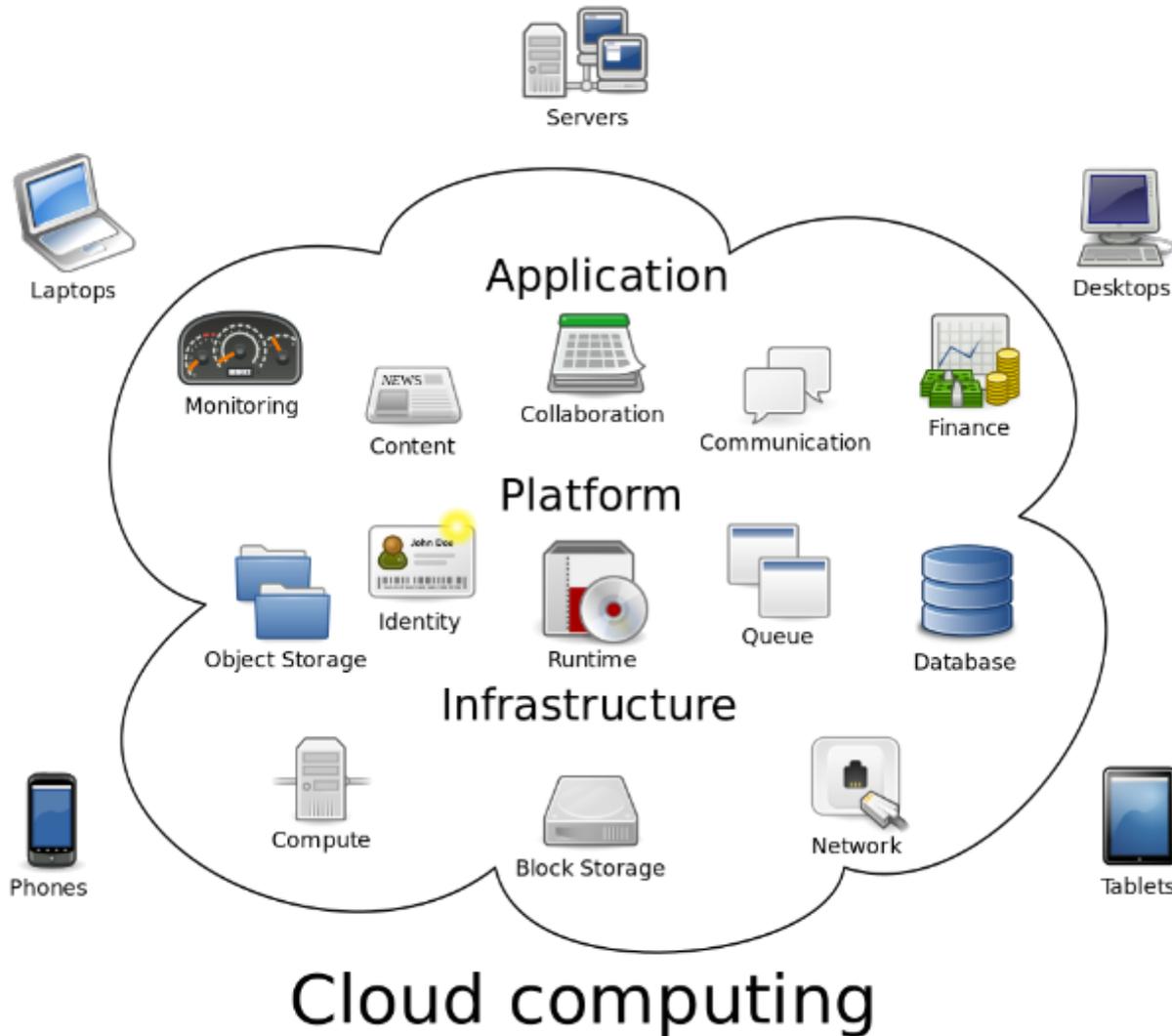
DEPSECDEF = Deputy Secretary of Defense, CIO = Chief Information Officer,
FRCS = Facility-Related Control Systems

Why The Cloud?

- The National Institute of Standards and Technology's (NIST) defines cloud in NIST Special Publication 800-145
- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction
- Five essential characteristics are inherent in the definition of cloud
 - On-demand self service
 - Broad network access
 - Resource pooling
 - Rapid elasticity
 - Measured service

What is The Cloud?

- The National Institute of Standards and Technology's (NIST) defines cloud in NIST Special Publication 800-145
- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction
- Five essential characteristics are inherent in the definition of cloud
 - On-demand self service
 - Broad network access
 - Resource pooling
 - Rapid elasticity
 - Measured service



https://en.wikipedia.org/wiki/Cloud_computing#/media/File:Cloud_computing.svg Created by Sam Johnston

Cloud Computing Service Models

- **IaaS** (Infrastructure as a Service), as the name suggests, provides you the computing infrastructure, physical or (quite often) virtual machines and other resources like virtual-machine disk image library, block and file-based storage, firewalls, load balancers, IP addresses, virtual local area networks etc. Examples: Amazon EC2, Windows Azure, Rackspace, Google Compute Engine.
- **PaaS** (Platform as a Service), as the name suggests, provides you computing platforms which typically includes operating system, programming language execution environment, database, web server etc. Examples: AWS Elastic Beanstalk, Windows Azure, Heroku, Force.com, Google App Engine, Apache Stratos.
- While in **SaaS** (Software as a Service) model you are provided with access to application software often referred to as "on-demand software". You don't have to worry about the installation, setup and running of the application. Service provider will do that for you. You just have to pay and use it through some client. Examples: Google Apps, Microsoft Office 365.

<https://stackoverflow.com/questions/16820336/what-is-saas-paas-and-iaas-with-examples>

DEPSECDEF Cloud Memo 2018

This cloud adoption initiative will occur in two phases. During phase one, DoD will use a tailored acquisition process to acquire a modern enterprise cloud services solution that can support unclassified, secret, and top secret information. This cloud services contract will also include, at a minimum, in-depth technical analysis of the current environment, the necessary cloud migration support, change management, and training. I am tasking the Director of DDS to lead phase one. During phase two, the CESG will rapidly transition select DoD Components or agencies to the acquired cloud solution, and, to the maximum extent possible, operationalize its mission using the security, software, and machine learning capabilities that cloud technology provides.

DIRECTOR OF NET ASSESSMENT
 DIRECTOR, STRATEGIC CAPABILITIES OFFICE
 DIRECTORS OF DEFENSE AGENCIES
 DIRECTORS OF DOD FIELD ACTIVITIES

SUBJECT: ACCELERATING ENTERPRISE CLOUD ADOPTION

Last month the Secretary of Defense visited Seattle, Washington, and Palo Alto, California, two epicenters of innovation in our country. That trip reflected several realities: (1) technologies in areas like data infrastructure and management, cybersecurity, and machine learning are changing the character of war; (2) commercial companies are pioneering technologies in these areas; and (3) the pace of innovation is extremely rapid. The Secretary is determined to prevent any potential adversary of the United States from surprising us or overtaking our military advantage. In that regard, I am directing aggressive steps to establish a culture of experimentation, adaptation, and risk-taking; to ensure we are employing emerging technologies to meet warfighter needs; and to increase speed and agility in technology development and procurement. While technological modernization has many dimensions, I believe accelerating the Department of Defense's (DoD's) adoption of cloud computing technologies is critical to maintaining our military's technological advantage. To that end, I am directing the following:

The Department will establish a Cloud Executive Steering Group (CESG) to devise and oversee the execution of a strategy to accelerate the adoption of cloud architectures and cloud services, focusing on commercial solutions. The CESG will report directly to the DSD. It will be chaired by Ellen Lord, Under Secretary of Defense for Acquisition, Technology, and Logistics (USD (AT&L)). The standing voting members of the CESG are Dr. Will Roper, Director of the Strategic Capabilities Office (SCO); Raj Shah, Managing Partner of the Defense Innovation Unit Experimental (DIUx); Chris Lynch, Director of the Defense Digital Service (DDS); and Joshua Marcuse, Executive Director of the Defense Innovation Board (DIB). John



This Statement of Objectives (SOO) describes the Department's intentions for the **Joint Enterprise Defense Infrastructure (JEDI) Cloud** program and for the supporting contract to **acquire commercial infrastructure as a service (IaaS) and platform as a service (PaaS) offerings.**

https://www.fbo.gov/index?s=opportunity&mode=form&id=f7f1d0314ec7c83cd0ace1636b5474a1&tab=core&_cvview=0 <

DEPSECDEF = Deputy Secretary of Defense

DoD CIO Cloud Policy

The screenshot shows a web browser window with the URL dodcio.defense.gov/Library/. The page is titled "POLICIES" and lists several key areas:

- DoD CIO Charter**
- Empower Mobile Data Access**
 - DoDI 8160.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense
 - DoDI 8420.01, Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies
- Modernize the Networks**
 - DoDD 8000.01, Management of the Department of Defense Information Enterprise
 - DoDI 8330.01, Interoperability of Information Technology (IT), Including National Security Systems
 - DoDI 8551.01, Ports, Protocols, and Services Management (PPSM)
- Share with Mission Partners**
 - DoDI 8110.01, Mission Partner Environment (MPE) Information Sharing Capability Implementation
 - DoDI 8220.02, Information and Communications Technology (ICT)
- Defend Against Cyber Attack**
 - DoDI 8205.10, Defense Industrial Base (DIB) Cyber Security/Information Assurance (CS/IA)
 - DoDI 8310.01, Information Technology Standards in the DoD
 - DoDI 8600.01, Cybersecurity
 - DoDI 8610.01, Risk Management Framework (RMF) for DoD Information Technology (IT)
 - DoDI 8520.02, Public Key Infrastructure (PKI) and Public Key (PK) Enabling
 - DoD 8535.01-M, "DoD Computer Network Defense-Service Provider Certification and Accreditation"
 - DoDI 8540.01, "Cross Domain (CD) Policy"
 - Department of Defense Cybersecurity Activities Performed for Cloud Service Offerings

Other sections visible include:

- ARCHITECTURES**: DOD Information Enterprise Architecture, DOD Architecture Framework, DoDAF V2.02
- OTHER PROGRAM**: DOD Information Resources Management Strategic Plan, DoD Privacy Impact Assessments (PIA)
- DOD IT BUDGET**: FY18 DoD IT Budget Request
- CYBERSECURITY AWARENESS**: Cybersecurity Awareness Month

<http://dodcio.defense.gov/Library/> CIO = Chief Information Officer

DoD CIO Cloud Policy

<http://dodcio.defense.gov/IntheNews/DoDInformationEnterpriseArchitecture.aspx>

DoD CIO Cloud Policy 2012



DEPARTMENT OF DEFENSE
 6030 DEFENSE PENTAGON
 WASHINGTON, D.C. 20301-6000

CHIEF INFORMATION OFFICER

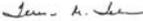
MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
 CHAIRMAN OF THE JOINT CHIEFS OF STAFF
 UNDER SECRETARIES OF DEFENSE
 DEPUTY CHIEF MANAGEMENT OFFICER
 COMMANDERS OF THE COMBATANT COMMANDS
 DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
 DIRECTOR, OPERATIONAL TEST AND EVALUATION
 GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
 INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
 ASSISTANT SECRETARIES OF DEFENSE
 ASSISTANTS TO THE SECRETARY OF DEFENSE
 DIRECTOR, ADMINISTRATION AND MANAGEMENT
 DIRECTOR, NET ASSESSMENT
 DIRECTORS OF THE DEFENSE AGENCIES
 DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense Cloud Computing Strategy

The Department is committed to realizing the value of cloud computing and providing a secure enterprise cloud environment, in alignment with Federal and Department-wide IT efficiency initiatives. The federal government intends to accelerate the pace at which the government will realize the value of cloud computing by requiring agencies to “evaluate safe, secure cloud computing options before making any new IT investments.” The attached DoD Cloud Computing Strategy lays the groundwork, consistent with the Federal Cloud Computing Strategy, for accelerating cloud adoption in the Department. The strategy includes steps to foster adoption of cloud computing, optimize data center consolidation, establish the DoD enterprise cloud infrastructure and continue to deliver cloud services. A robust and resilient multi-provider, Enterprise Cloud Environment will enable the Department to achieve the goals of the Joint Information Environment.

An implementation plan will follow, which will include further detail. In addition, a communications plan will promote the “Enterprise-first” approach to cloud computing and the use of a DoD Enterprise Cloud Services Broker, and address the cultural challenges associated with the adoption and implementation of cloud services. The existing Cloud Computing Working Group, led by the DoD CIO and the Defense Information Systems Agency, will continue to support follow-on strategy efforts.

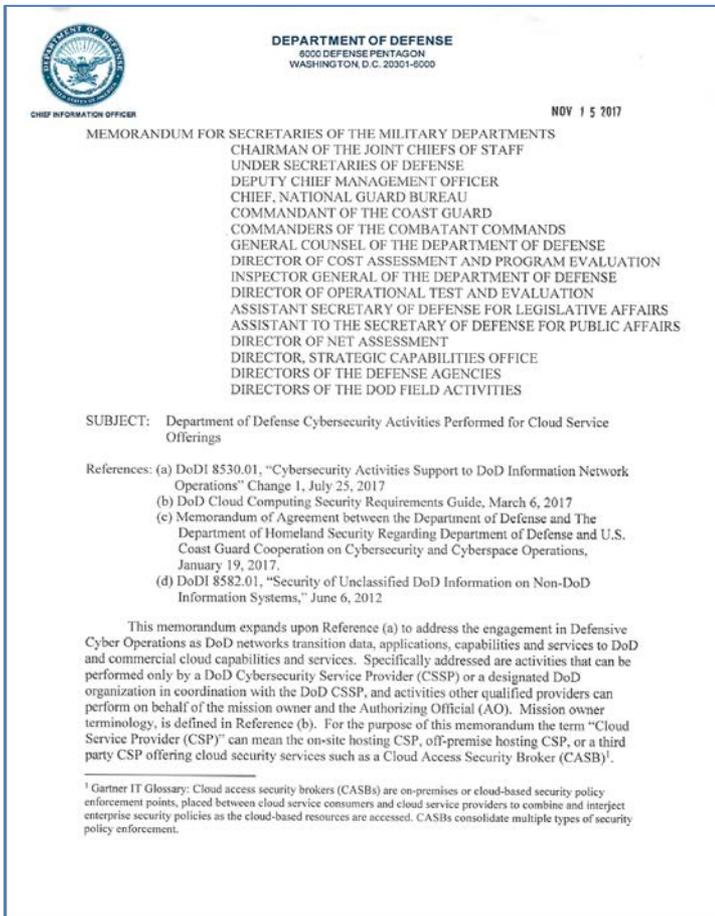
The DoD CIO point of contact for DoD Cloud Computing is Mr. Robert Vietmeyer at email: robert.vietmeyer@osd.mil, 571-372-4461.


 Teresa M. Takai

Attachment:
As stated

- *Accelerate cloud adoption*
- *Optimize data center consolidation*
- *Establish DoD Cloud enterprise cloud infrastructure*
- *Continue to deliver cloud services*

DoD CIO Cybersecurity Cloud Offerings 2017



- Mission owners are required to register DoD networks, applications, data, and services that are migrating to DoD and/or commercial cloud capabilities and services.
- Required to identify the cloud service provider's alignment to an appropriate DoD CSSP in the DoD CIO System/Network Approval Process (SNAP) database.
- Mission owner is responsible for ensuring data migrated to a DoD or commercial cloud is at the appropriate security impact level

EO 13556 Controlled Unclassified Information

- Executive Order 13556 "Controlled Unclassified Information" 2010
- Established by Executive Order 13556, the Controlled Unclassified Information (CUI) program standardizes the way the Executive branch handles unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies.
- Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

DFARS Safeguarding CUI 2015

Guidance to Stakeholders for Implementing
Defense Federal Acquisition Regulation Supplement
Clause 252.204-7012
(Safeguarding Unclassified Controlled
Technical Information)



Version 2.0

August 2015

Office of the Deputy Assistant Secretary of Defense for Systems Engineering
Washington, D.C.

Distribution Statement A: Approved for public release.

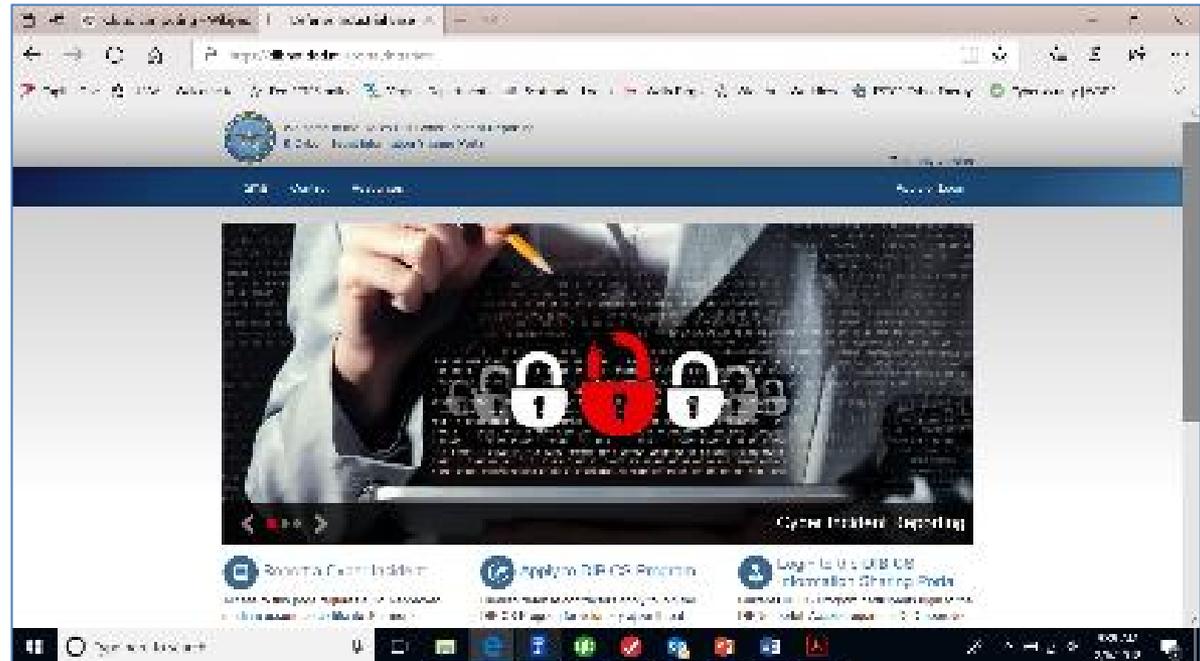
- Intended for stakeholders charged with protection of unclassified controlled technical information (CTI) resident on or transiting through contractor information system(s)
- CTI is technical information with military or space application that is subject to controls on its access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.
- This guide will assist stakeholders in carrying out their responsibilities should a defense contractor report a compromise on a contract that contains unclassified CTI.

DFARS Safeguarding CUI 2015

Appendix F. Incident Collection Format (ICF) Template

- 1.) UNCLASSIFIED/ FOR OFFICIAL USE ONLY (when filled in)
- 2.) FOR INTERNAL USE ONLY
- 3.) Report ID: xxx-xxxxx
- 4.) Company Name: xxxxx
- 5.) DUNS Number: xxxxx
- 6.) Contract Number Affected (Additional contract numbers can be added on a subsequent page):
xxxxxx-xx-x-xxxx
- 7.) Contract Clearance Level: xxxxxx
- 8.) Facility CAGE Code: xxxxx
- 9.) Does this incident affect cloud services provided to DoD?: xx
- 10.) Does this incident impact unclassified controlled technical information as defined in DFARS clause 252.204-7012?: xxx
- 11.) Last Name: Xxxxxxx
- 12.) First Name: Xxxxxxx
- 13.) Position Title: xxxxxxxxxxxx
- 14.) Location: xxxxxxxxxxxxxxxxx
- 15.) City: xxxxxxxxxxxxx
- 16.) State: xxxxxxxxxxxxxx
- 17.) Postal Code: xxxxx
- 18.) Telephone: xxx-xxx-xxxx
- 19.) E-mail Address: xxxxxx.xxxxx@xxxxxx.xxx
- 20.) Subcontractor Name [if incident was on a subcontractor network]: xxxxx
- 21.) Subcontractor CAGE Code: xxxxxx

Guidance to Stakeholders for Implementing DFARS 252.204-7012
22



3.1.1 DFARS Cyber Incident Reports

DFARS cyber incidents are reported to the Defense Cyber Crime Center (DC3) via the DIBNet [portal](#)⁴. Note: DIBNet is a web portal for sharing threat information between DoD and DIB companies. See appendix F for a list of reportable fields.

If the contractor does not have all the information required by the clause within the 72-hour time constraint, specified in paragraph (d)(1) of the safeguarding clause, the contractor should report the details available at the time.

DISA Cloud Computing SRG V3 2017

<ul style="list-style-type: none"> Cloud Computing Security Requirements Guide 1 INTRODUCTION 2 BACKGROUND 3 INFORMATION SECURITY OBJECTIVES IMPACT LEVELS 4 RISK ASSESSMENT OF CLOUD SERVICE OFFERINGS 5 SECURITY REQUIREMENTS 6 CYBERSPACE DEFENSE AND INCIDENT RESPONSE Appendix A - References Appendix B - Glossary Appendix C - Roles and Responsibilities Appendix D - CSP Assessment Parameter Values for FA Appendix E - Privacy Overlay Comparative OIG Tables and Value Tables Appendix F - FUTURE Privacy Overlay Guidance List of Tables List of Figures 	  <p>Department of Defense Cloud Computing Security Requirements Guide Version 1 Release 3 6 March 2017</p> <p><small>Developed by the Defense Information Systems Agency for the Department of Defense</small></p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Trademark Information Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by DoD, DISA, the DISA Risk Management Executive (RME), or DISA RME Cybersecurity Standards Branch of any non-Federal entity, event, product, service, or enterprise.</p> </div>
--	---

1 Introduction

[Question/Comment](#) [Send this link](#)

Cloud computing technology and services provide the Department of Defense (DoD) with the opportunity to deploy an Enterprise Cloud Environment aligned with Federal Department-wide Information Technology (IT) strategies and efficiency initiatives. Cloud computing enables the Department to consolidate infrastructure, leverage commodity IT functions, and eliminate functional redundancies while improving continuity of operations. The overall success of these initiatives depends upon well executed security requirements, defined and understood by both DoD Components and industry. Consistent implementation and operation of these requirements assures mission execution, provides sensitive data protection, increases mission effectiveness, and ultimately results in the outcomes and operational efficiencies the DoD seeks.

The 15 December 2014 DoD CIO memo regarding Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services defines DoD Component responsibilities when acquiring commercial cloud services. The memo allows components to responsibly acquire cloud services minimally in accordance with the security requirements outlined in Federal Risk and Authorization Management Program (FedRAMP) and this Cloud Computing Security Requirements Guide (CC SRG). Defense Information Systems Agency (DISA) previously published the concepts for operating in the commercial cloud in the Cloud Security Model. Version 1 defined the overall framework and provided initial guidance for public data. Version 2.1 added information for Controlled Unclassified Information. The CC SRG documents cloud security requirements in a construct similar to other SRGs published by DISA for the DoD. This SRG incorporates, supersedes, and rescinds the previously published Cloud Security Model (CSM).

1.1 Key Terms

[Question/Comment](#) [Send this link](#)

This CC SRG introduces terminology and concepts that are unique to cloud computing and DoD's usage of the technology. While this section lists some of the key terms, please refer to Appendix B: Glossary for their definitions before, or as, reading this document to realize a full understanding of the content and requirements. The following is a list of key terminology which is used throughout this document:

- Cloud Service Provider (CSP)

- SRG outlines the security model by which DoD will leverage cloud computing along with the security controls and requirements necessary for using cloud-based solutions.
- SRG applies to DoD provided cloud services and those provided by a contractor on behalf of the Department.

DISA Cloud Computing SRG

The CC SRG serves several purposes

- Provides security requirements and guidance to DoD and commercial Cloud Service Providers (CSPs) (DoD contractors) that wish to have their Cloud Service Offerings CSO(s) included in the DoD Cloud Service Catalog.
- Establishes a basis on which DoD will assess the security posture of a DoD or non-DoD CSP's CSO, supporting the decision to grant a DoD Provisional Authorization (PA) that allows a CSP to host DoD missions.
- Establishes a basis on which a DoD Component's Authorizing Official (AO) will assess the security posture of a DoD CSP's CSO, supporting the decision to grant a DoD Component's Authorization to Operate (ATO) for the CSP/CSO, and a DoD PA if the CSO might be leveraged by other DoD Components. (e.g., DISA's ATO/PA for milCloud)

DISA Cloud Computing SRG (Cont'd)

- Defines the requirements and architectures for the use and implementation of DoD or commercial cloud services by DoD Mission Owners.
- Provides guidance to DoD Mission Owners, Security Control Assessors (SCA), Authorizing Officials, (formerly Certification and Accreditation (C&A) officials), and others in planning and authorizing the use of a CSO.
- Supports the DoD Chief Information Officer's (CIO) Cloud initiative to migrate DoD web sites and applications from physical servers and networks within DoD networks and data centers into lower cost commodity IT services which typically include virtual servers and networks that are an integral part of most cloud services provided by both DoD and commercial CSPs.
- Supports the DoD CIO's and Federal Government's Data Center Reduction initiatives.

DISA Cloud Computing SRG

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

NOTE: See Section 5.2.1, *Jurisdiction/Location Requirements* for the explanation of "US / US outlying areas"

NOTE: ADP-1 and ADP-2 Personnel Requirements apply to both impact levels 4 and 5. See 5.6.2, .1,.2,.3

NOTE: Level 4/5 off-premises CSO connectivity will be via a BCAP on any DISN network (e.g., DREN) it serves.

Figure 1 – Impact Level Comparison

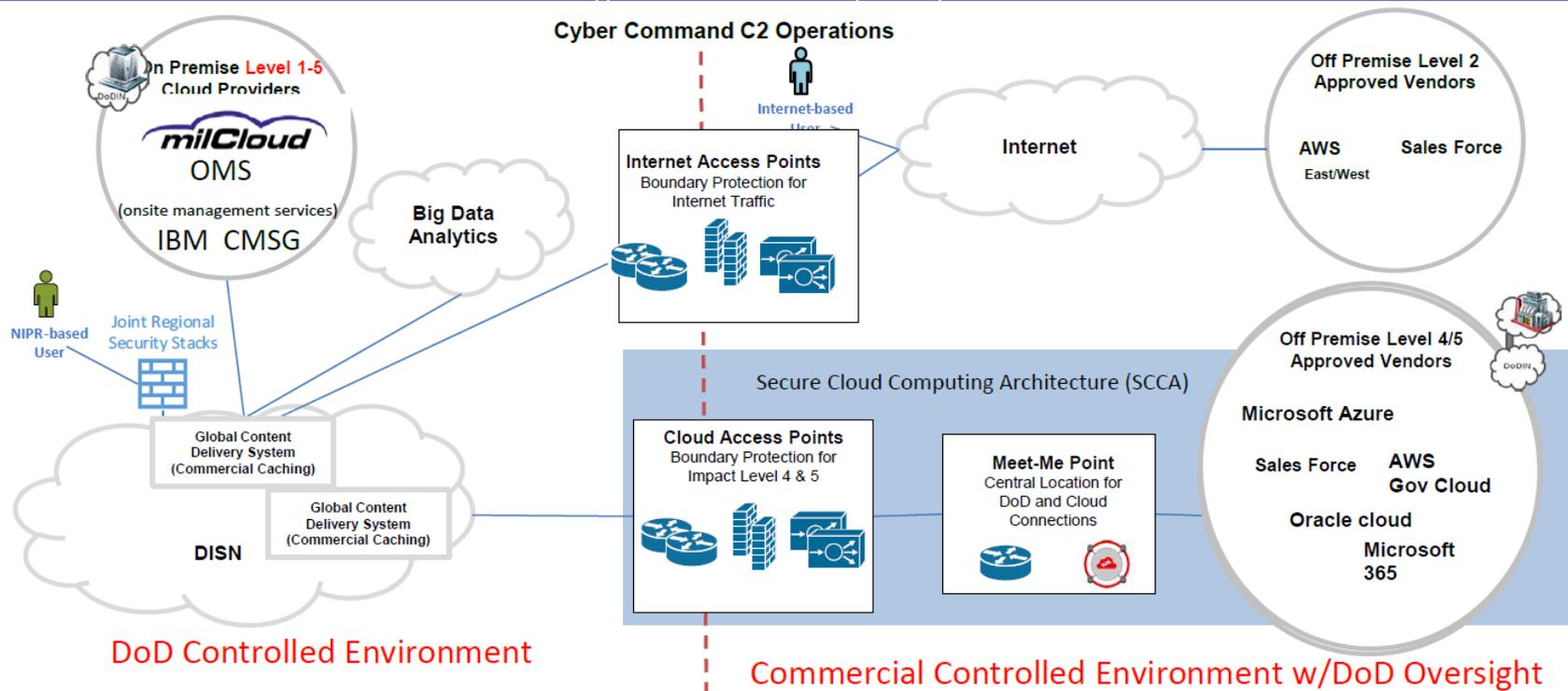
DISA-DoD Cloud Deployment



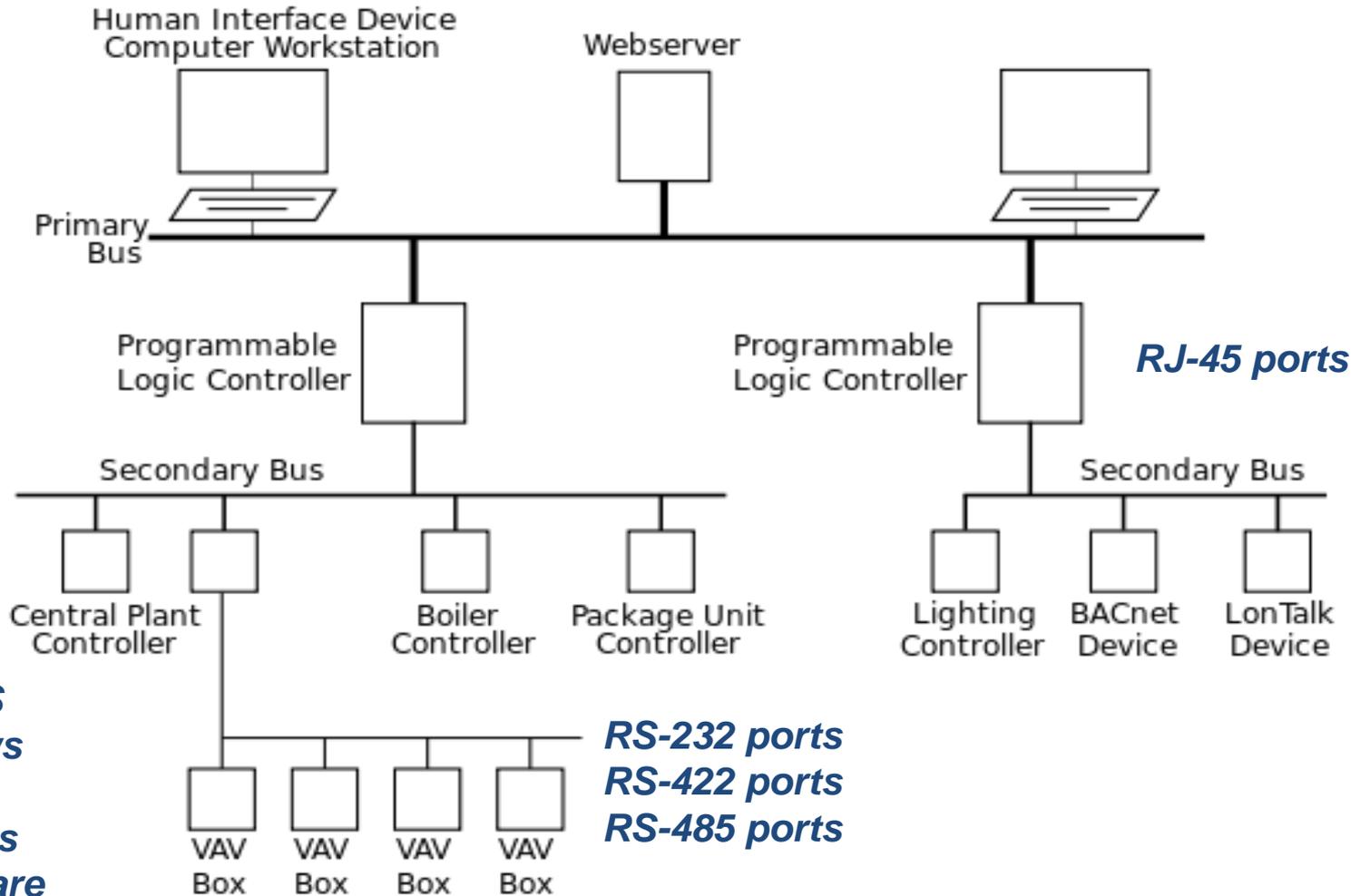
Unclassified DoD Commercial Cloud Deployment Approach

UNCLASSIFIED

Vendors named within are approved or under contract to provide specified services to DISA or DOD



FRCS Traditional Architecture



QNX OS
Windows
CE
VxWorks
Microware
Others

RS-232 ports
RS-422 ports
RS-485 ports

FRCS = Facility-Related Control Systems

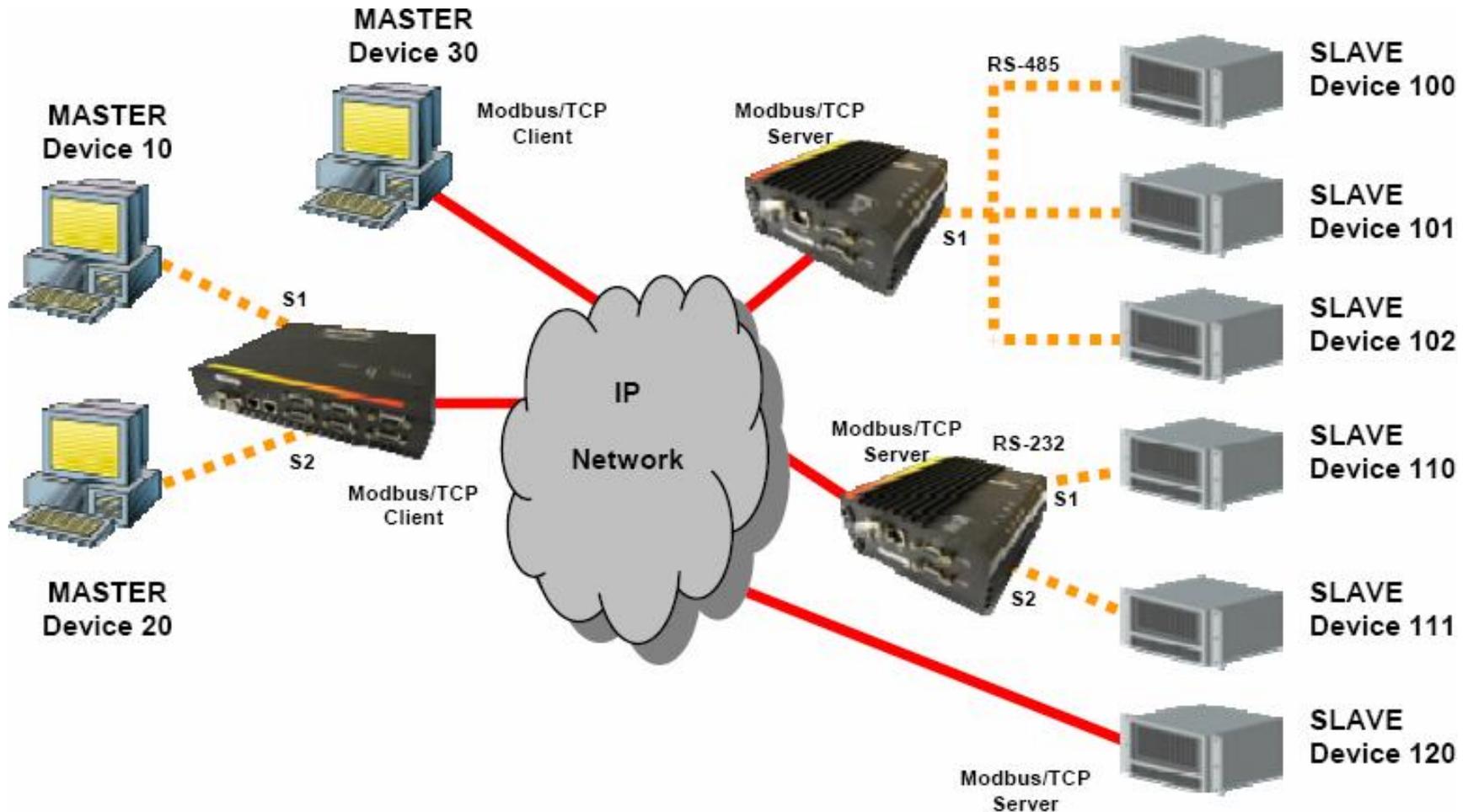
FRCS Traditional Architecture

- Traditional FRCS Client-Server Architecture
- Vast majority of FRCS are organization owned client-server architecture
- Systems can last 15-20 years
- Probably 80% or more of the legacy systems are running Windows 95, XP, CE
- Many have hardcoded passwords or no passwords at device level
- Level 4 servers and workstations can be virtualized, and some Level 3 FPOC's controllers can support some logging

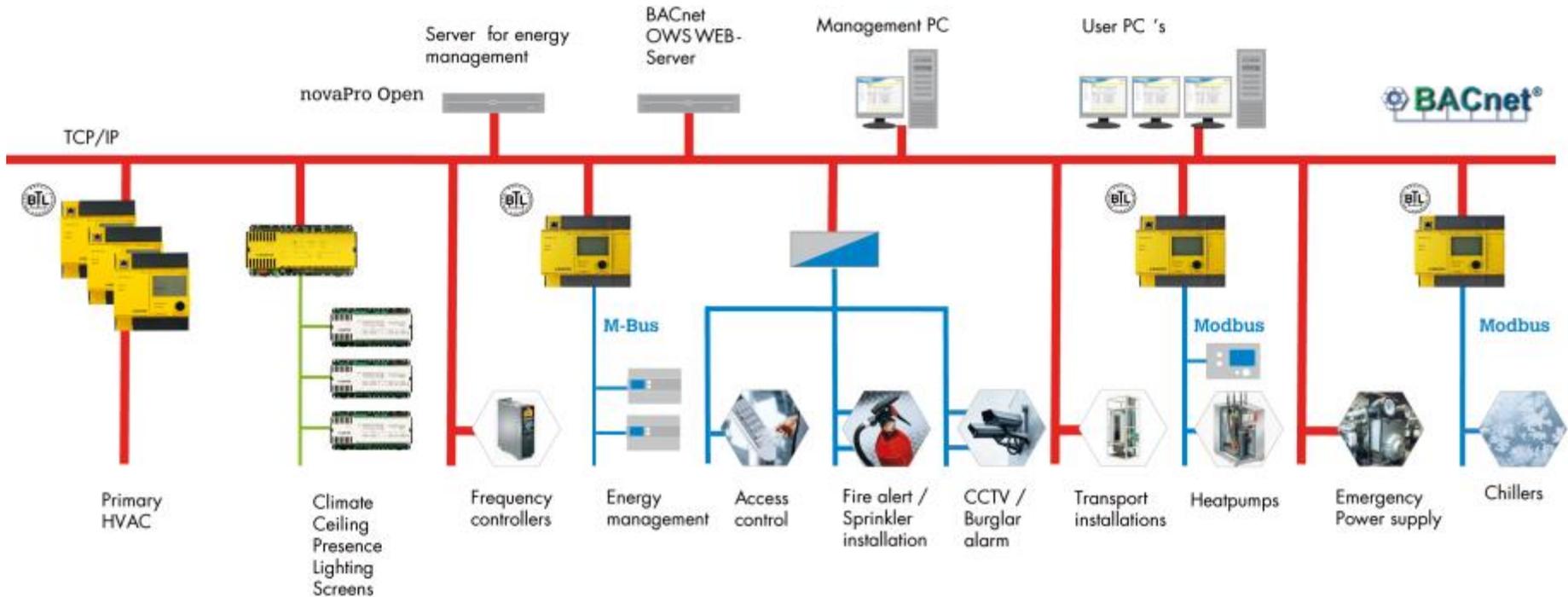
Cloud Architectures

- Smart buildings/cities are moving to cloud architectures at a rapid pace
- Manages the building functions, energy, tenant data very efficiently
- Controllers still need to be in the Levels 3-0 physical space; Level 4 can be in cloud space
- Cloud security is typically much better than organization owned client-server architecture; they follow NIST RMF, conduct continuous monitoring, multi-factor authentication can be enabled
- If network connectivity is lost, controllers default to safe mode

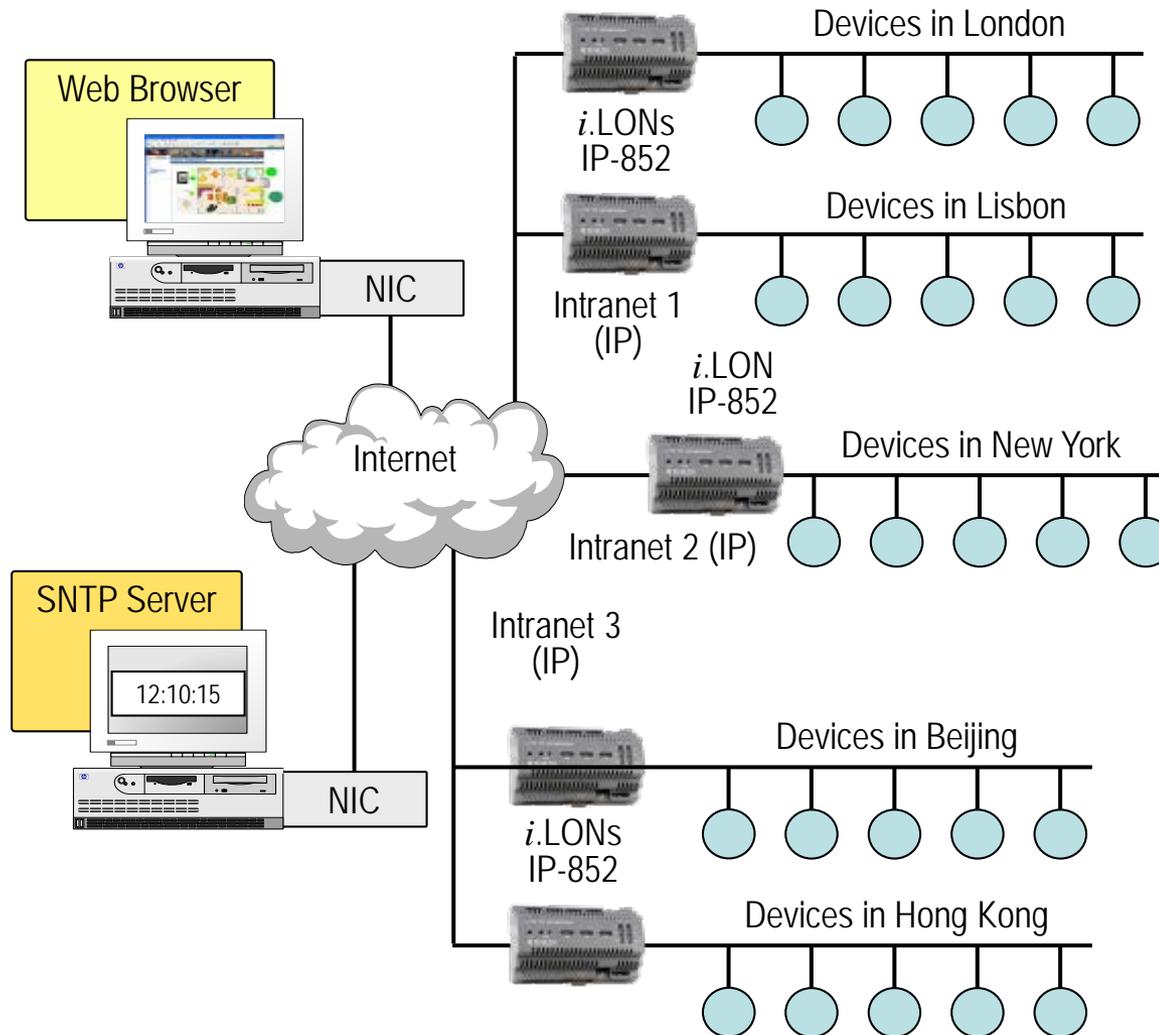
FRCS Traditional Modbus Architecture



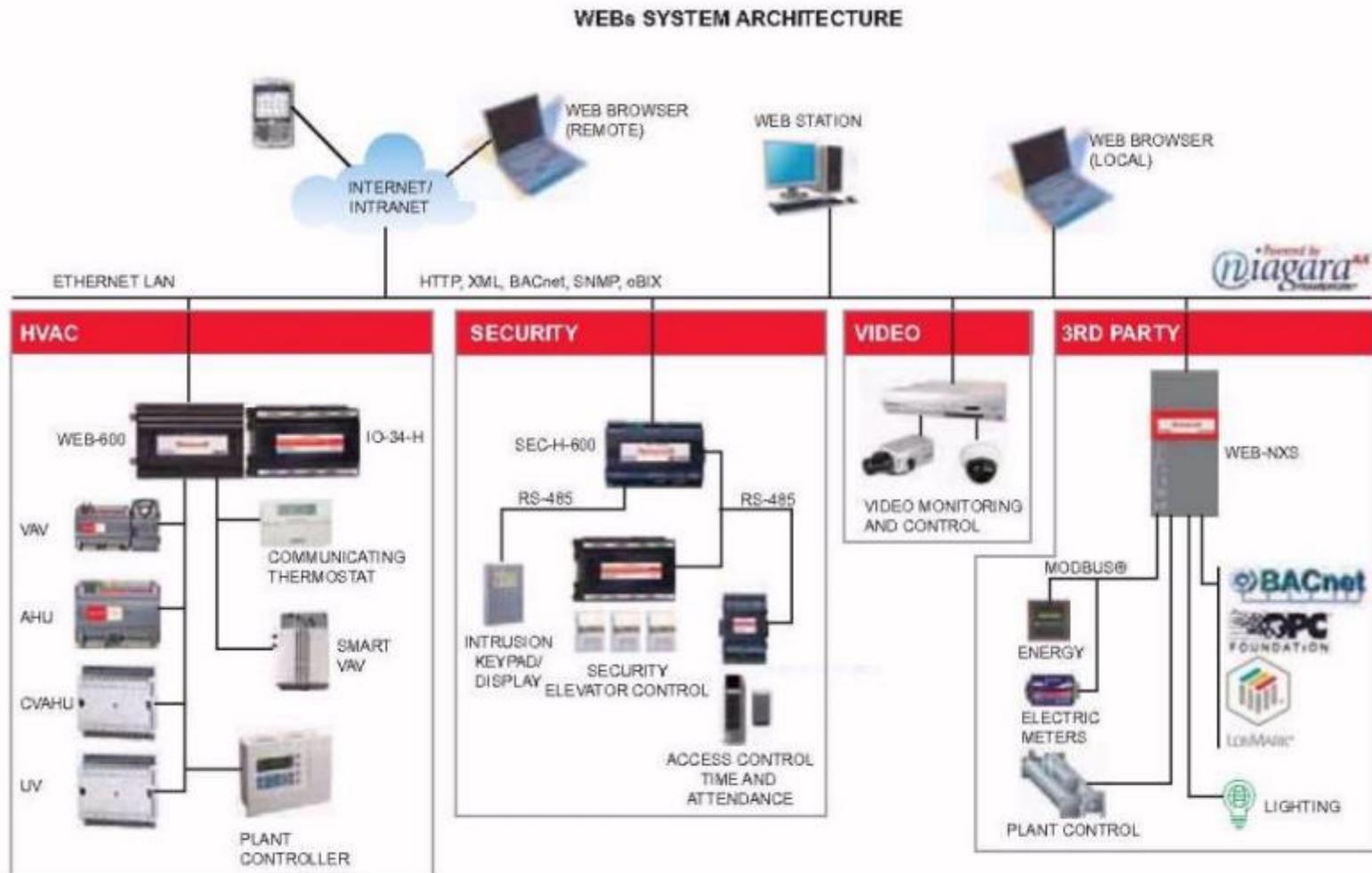
FRCS Traditional BACNet Architecture



FRCS Traditional Lonworks Architecture

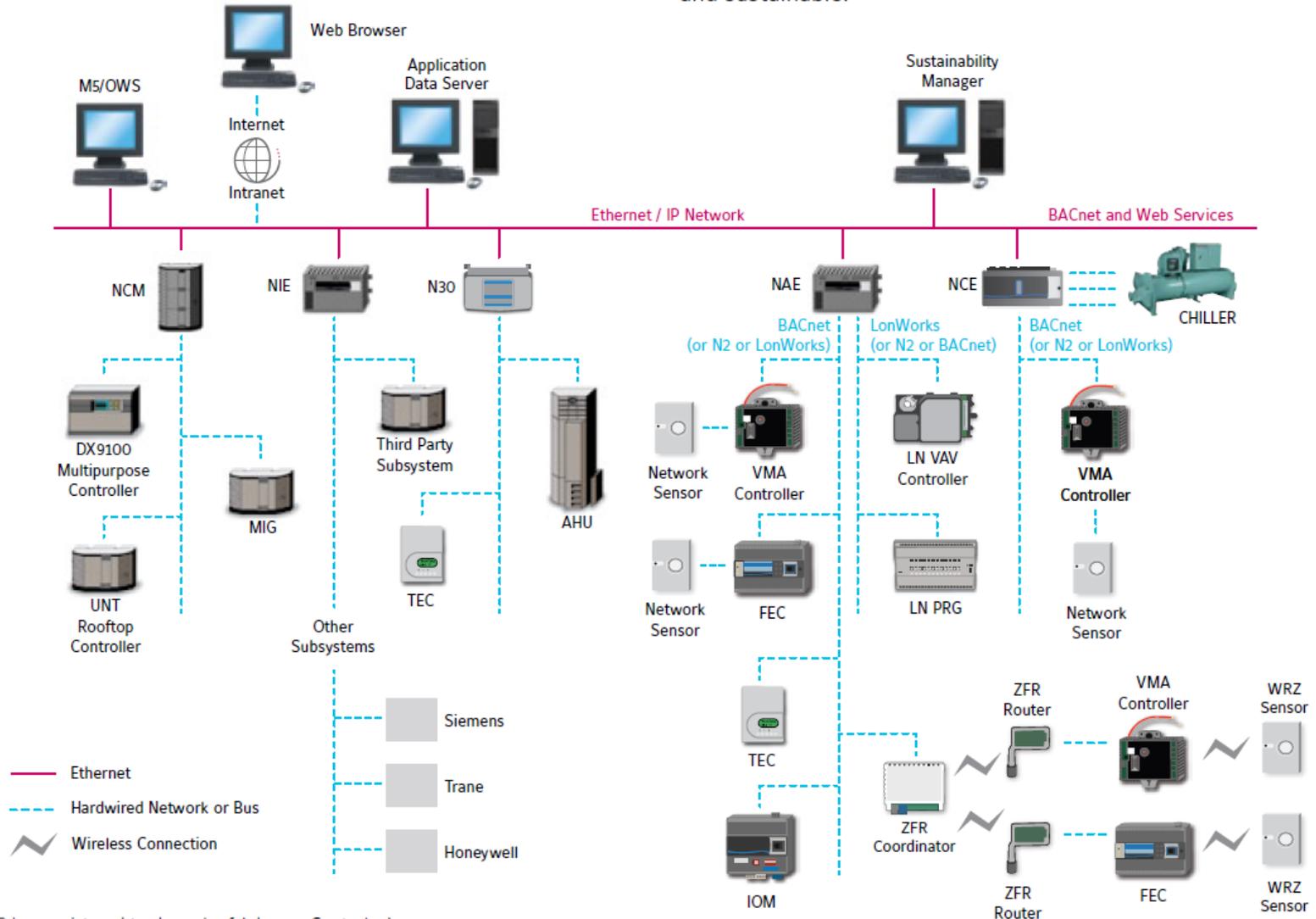


FRCS Traditional Tridium Architecture



FRCS Traditional Johnson Architecture

and sustainable.

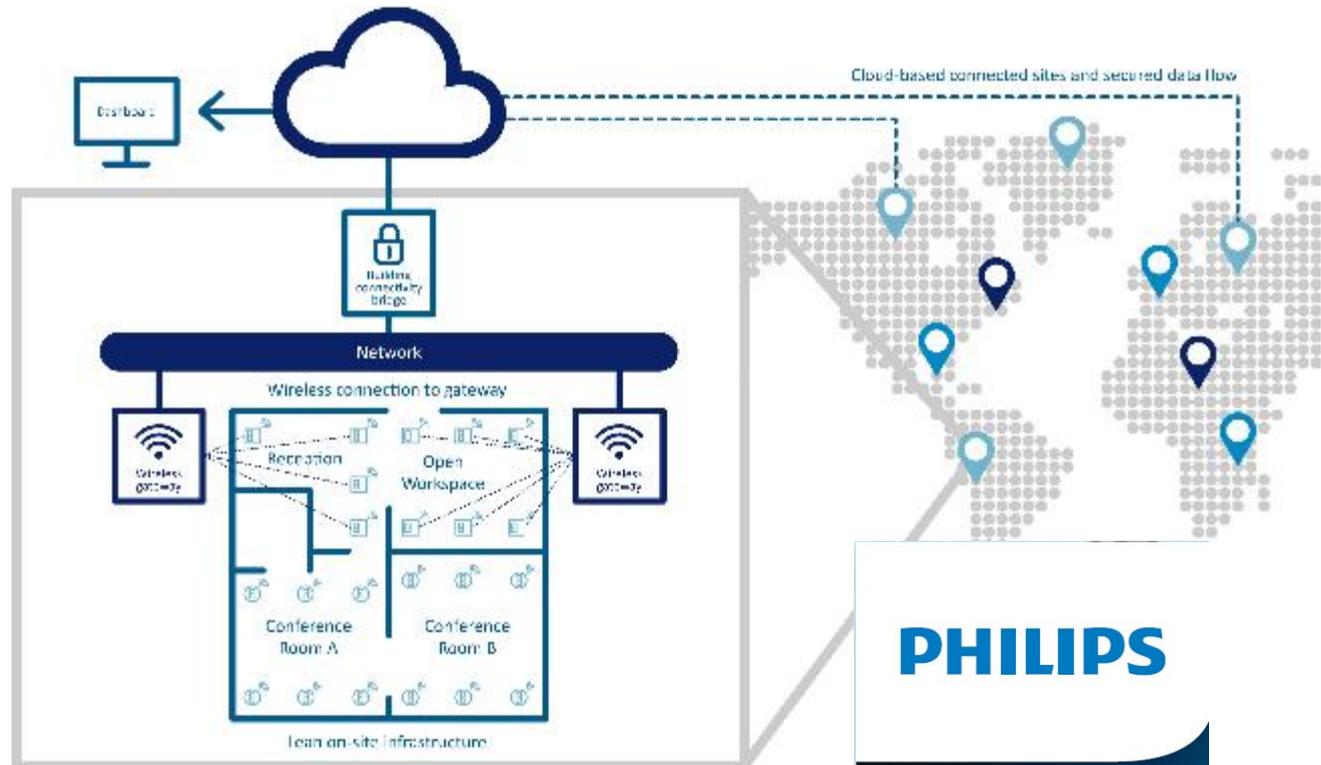


Industry Transformation – LaaS

Lighting that connects your space to the cloud

A lean on-site hardware infrastructure that allows for future upgrades and expansion

A cloud-based system enabling virtually unlimited growth of connected sites and data flow

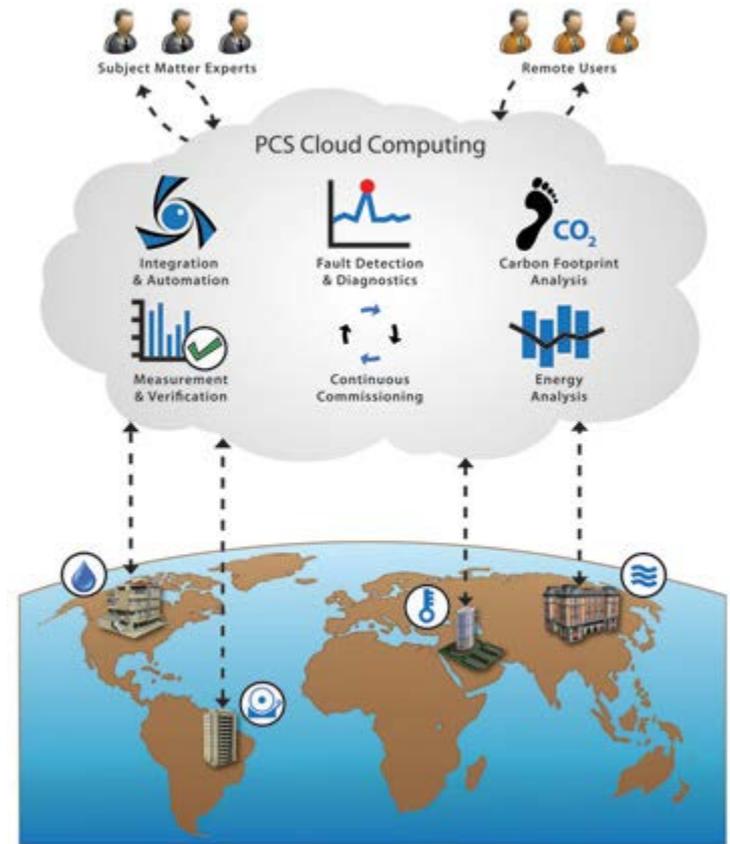
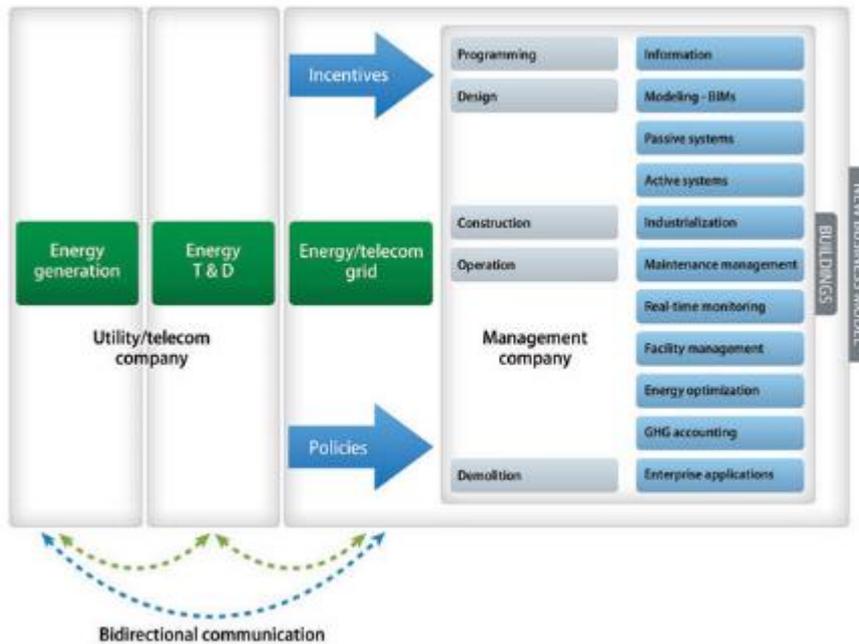


PHILIPS

InterAct Office

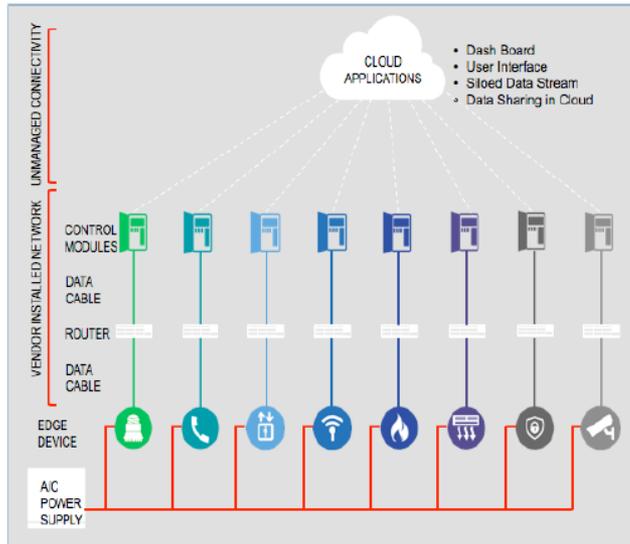
Smart buildings

Industry Transformation – Smart Buildings



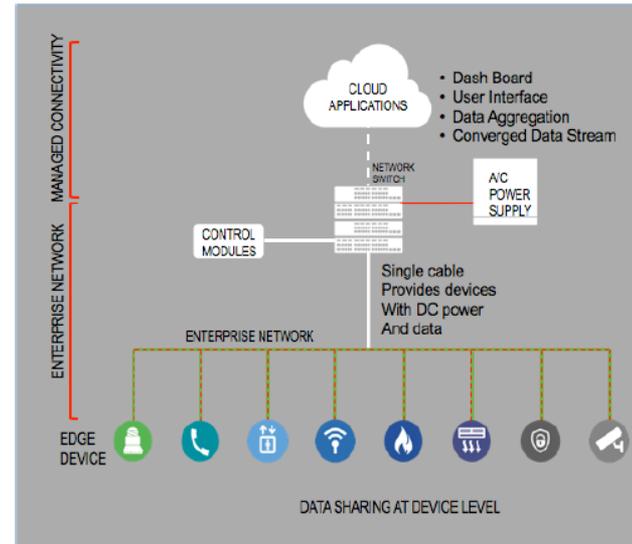
<http://www.pacificcontrols.net/solutions/ict.html>

Industry Transformation – PoE



Traditional System Diagram
Figure 1

- Multiple and redundant infrastructures to distribute power and data to edge devices
- Vendor-installed networks can create security risks
- Data sharing only happens at an enterprise level



Cisco Digital Building Diagram
Figure 2

- Single infrastructure to distribute power and data to edge devices
- Enterprise-level network for all systems
- Data sharing is available at the



Cloud Pros and Cons

Pros	Cons
Managed Services and Continuous Monitoring provide high level of data security (when done right), assumed internet connection always available	Shared responsibility between CSP and User, User needs to conduct monthly audits of System, Applications and Users; OT Level 3 and below default to Safe Mode
Very High Data Center Physical Security	User still needs equivalent physical security safeguards at local site; a dedicated SOC/BOC/FEOC
Mature threat, intelligence and SEIM tools, patching and AV/Malware services	User still needs to understand and use the tools, skilled IT/OT staff hard to find
Multiple data backups and recovery sites	User still needs to manage the IR and DR functions, limits on out of US data, a dedicated SOC/BOC/FEOC
VM environments allows rapid spin-up/spin-down of instances	Users can expose data and systems if not configured properly (e.g. Amazon S3)
Easy to segregate DoD data in Virtual Private Clouds	User still responsible for data security
Cost is generally much less than owning, managing hw/sw, dynamic pricing models	User has relinquished control of the physical infrastructure
Easy to segregate DoD data in Virtual Private Clouds	User still responsible for data security
Cost is generally much less than owning, managing hw/sw, dynamic pricing models	User has relinquished control of the physical infrastructure

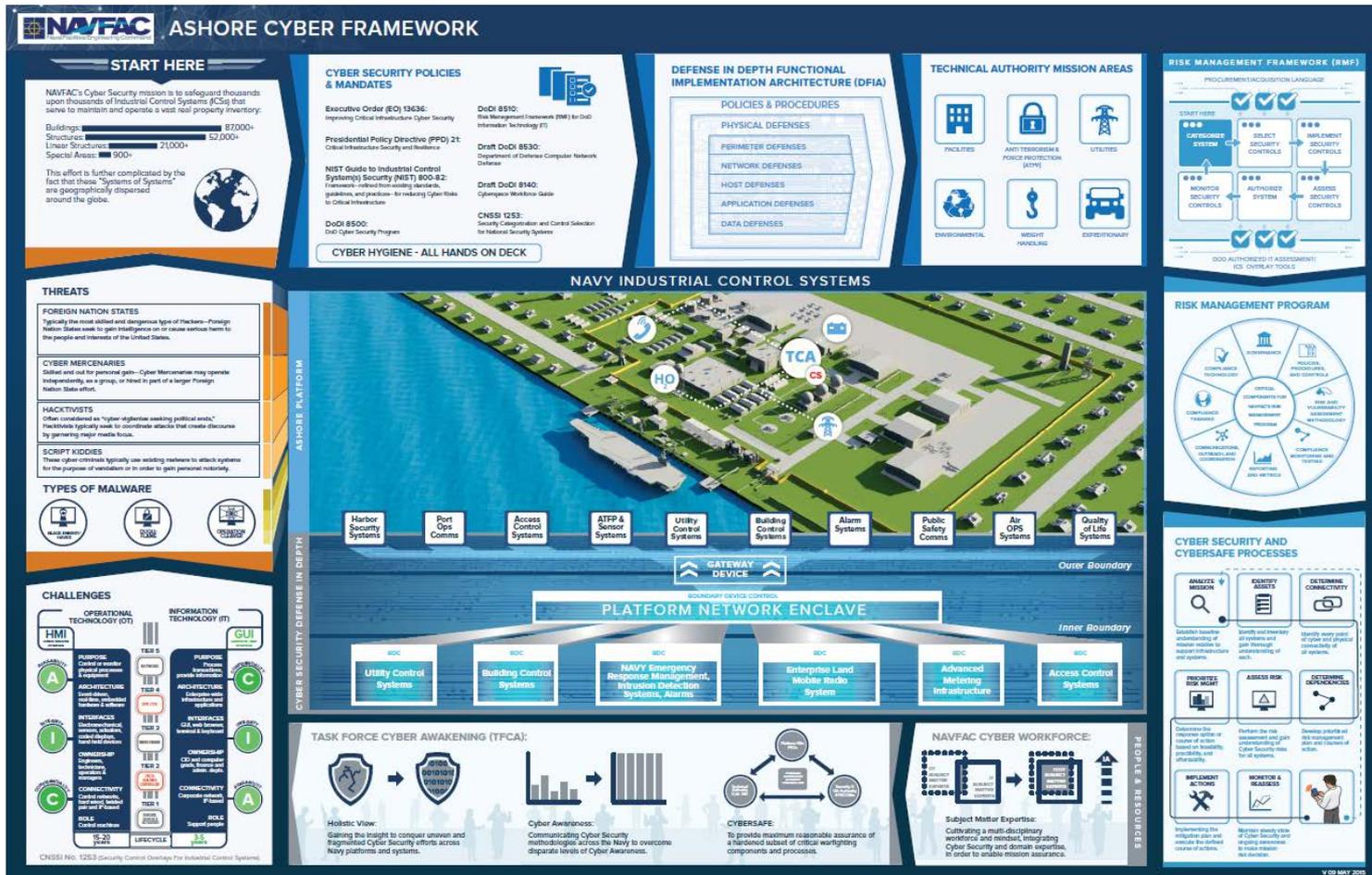
FRCS Cyber Ranges

- The current Cyber Ranges can only provide a very small capability to exercise FRCS, typically only on the PE IT Front-End. The sheer number of OA devices and components, vendor/suppliers, and combinations of system integrations makes it almost impossible to model or mimic a real world production FRCS. For example, a single building may have a Tridium and Johnson Control Utility and Monitoring Control System, a Honeywell Fire Alarm & Life Safety System, a Bosch Electronic Security System, and an Otis Vertical Transport System and 100,000 plus individual controllers (HVAC, lighting, fire and smoke detectors, elevator, etc.). Unlike IT systems, the FRCS controllers do not typically run Windows or Linux OS, and do not use x86 chip sets, and are therefore not capable of being properly modeled in the current TDE and Cyber Range environments.
- The current effort is to create small physical mini-systems TDE's and Test Beds that replicate one, two or three of the systems with the PE and the OA components such as the UMCS, FLS and ESS. These efforts will suffice for the next 3-5 years to begin to train and educate the IT and OT workforce on how to detect, mitigate and recover FRCS, but in the long-term, will be cost prohibitive and unsustainable.

Cloud FRCS Challenges

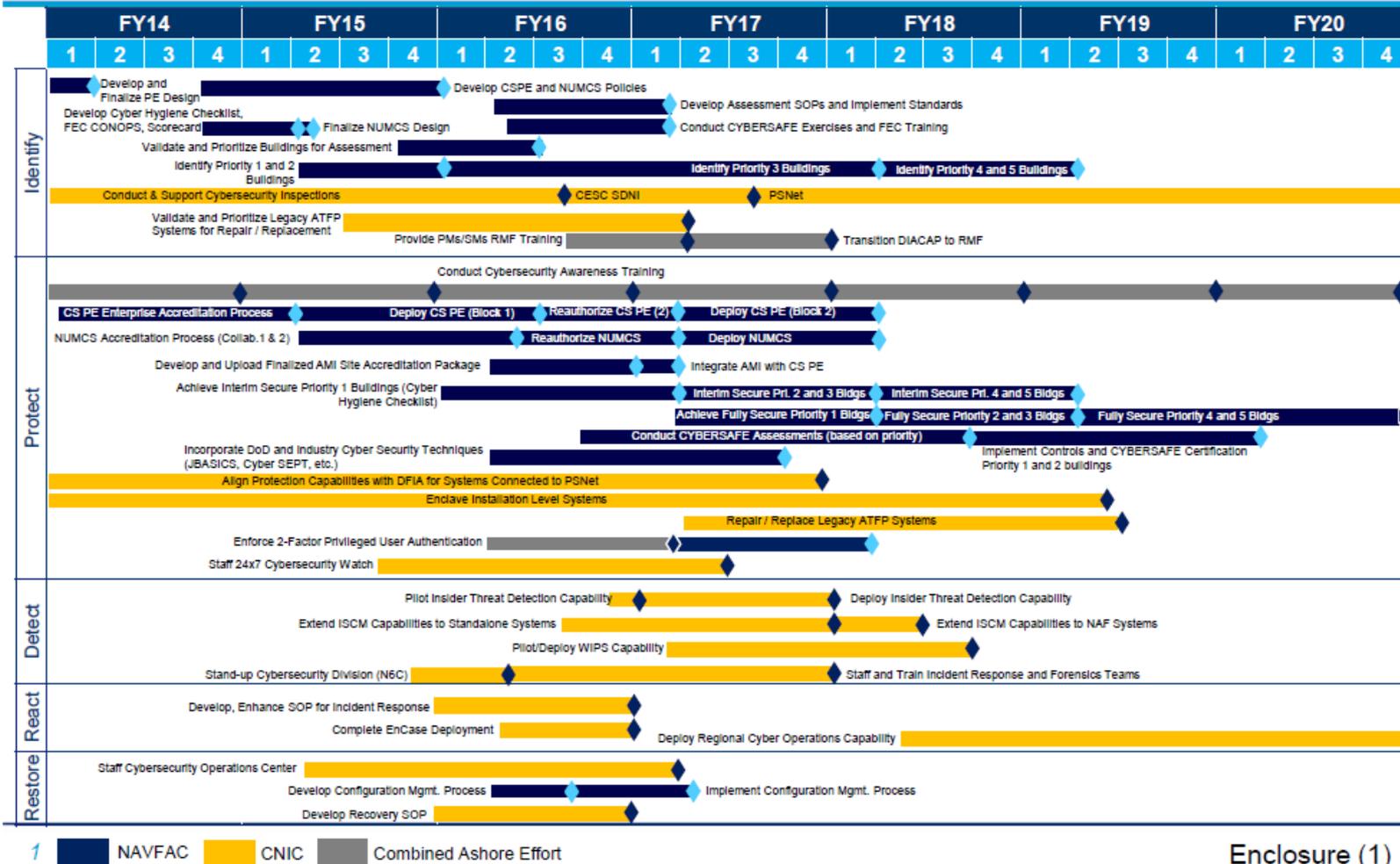
- Virtualization of FRCS controllers with OS such as QNX, WindowsCE, and chip sets such as Texas Instruments and Motorola so that a software defined network and FRCS can be generated with drop and drag objects in Visio or exercise tools
- Visualization of FRCS in 4 dimensional space and time, and the capability to integrate into Computerized Maintenance Management Systems (CMMS) tools (Maximo, Tririga, Archibus, etc.) and the DoD BUILDER tool
- Use of Virtual Reality and Augmented Reality to allow the Facility Operations Center defenders and analysts to have real-time situational awareness and the criteria to identify normal operations and behavior from abnormal behavior and/or active exploit/attack
- Configuration Management and exercise methodologies to enable the exercise team to quickly prepare the Red and Blue Team Playbooks, monitor exercise execution offense and defense, provide exercise evaluation to participants, and reset the TDE or Range back to baseline

Navy Ashore Cyber Framework





Navy Ashore Domain Cybersecurity Plan



Enclosure (1)



Unclassified

Warfighting First – Operate Forward – Be Ready



CYBERSAFE Instruction



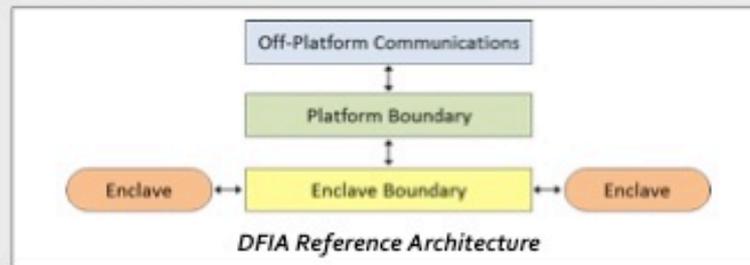
CYBERSAFE Instruction

Establishes policy and assigns responsibilities for the management and implementation of Navy Cybersecurity Safety (CYBERSAFE) Program requirements

- Assigns responsibility for management and implementation of CYBERSAFE Program
- Describes 3 Facets of CYBERSAFE
 - Cyber System Levels → Design
 - CYBERSAFE Grades → Procure & Build
 - Cyber Conditions of Readiness → Operate
 - IT / IA TAB will determine method for leveraging Facets and Platform Architecture to consistently identify CYBERSAFE critical items
- Identifies management controls for CYBERSAFE items
- Describes CYBERSAFE Technical, Certification, and Threat/Risk Assessment Authorities
- Depicts Defense-in-Depth architecture as defined by DFIA *
 - DFIA details control point strategy, but will also define DiD Implementation Standards across cyber environment

Cyber System Level	CYBERSAFE Grade
CSL 1: Platform Safety	Grade A: Mission Critical
CSL 2: Platform Combat	Grade B: Mission Essential
CSL 3: Networked Combat	Grade C: Non-Mission Essential
CSL 4: Sustained Combat	

Cyber Condition	Mission Capability																		
<table border="0"> <tr> <td></td> <td>Tech Capabilities</td> </tr> <tr> <td>X FULL NET</td> <td>.....</td> </tr> <tr> <td>Y SEMI NET</td> <td>.....</td> </tr> <tr> <td>Z NO NET</td> <td>.....</td> </tr> </table>		Tech Capabilities	X FULL NET	Y SEMI NET	Z NO NET	<table border="0"> <tr> <td></td> <td>Ops Capabilities</td> </tr> <tr> <td>Fight Ready</td> <td>.....</td> </tr> <tr> <td>Fight Hurt</td> <td>.....</td> </tr> <tr> <td>Fight Alone</td> <td>.....</td> </tr> <tr> <td>Get Home</td> <td>.....</td> </tr> </table>		Ops Capabilities	Fight Ready	Fight Hurt	Fight Alone	Get Home
	Tech Capabilities																		
X FULL NET																		
Y SEMI NET																		
Z NO NET																		
	Ops Capabilities																		
Fight Ready																		
Fight Hurt																		
Fight Alone																		
Get Home																		



* DFIA: Defense-in-Depth Functional Implementation Architecture

Virtual Power Station for Naval Facilities

ESTCP Number: EW18-D2-5307 *Centralized market integration and cyber situational awareness for revenue capture and a joint, national-level DoD energy ICS cyber capability*

- This project will **implement a commercial VPS within the DoD's unique cybersecurity environment**. It will connect the **electricity sector-specific IT security services** offered by the Electricity Information Sharing and Analysis Center (E-ISAC) and the IT analytics provided by the Lincoln Research Network Operations Center (LRNOC). The VPS system will then **demonstrate increased energy asset awareness (both load and generation), operational economic savings, and a strengthened cybersecurity posture** through a demonstration with Navy Region Mid-Atlantic and Naval Station Norfolk. As a centralized solution that builds capability on top of Naval Facilities Engineering Command's (NAVFAC) existing Public Safety Network (PS-NET) and Facilities Engineering and Operations Cell (FEOC), a primary objective for the VPS design is integration with every FEOC and installation in the NAVFAC enterprise. The team's goal is to eventually **turn the Navy VPS into a joint, national-level operational capability serving the entire DoD installation enterprise**. To this end, the project team will position the VPS system for reciprocity by other services through **rigorous RMF controls traceability documentation** and stakeholder engagement.

Virtual Power Station for Naval Facilities

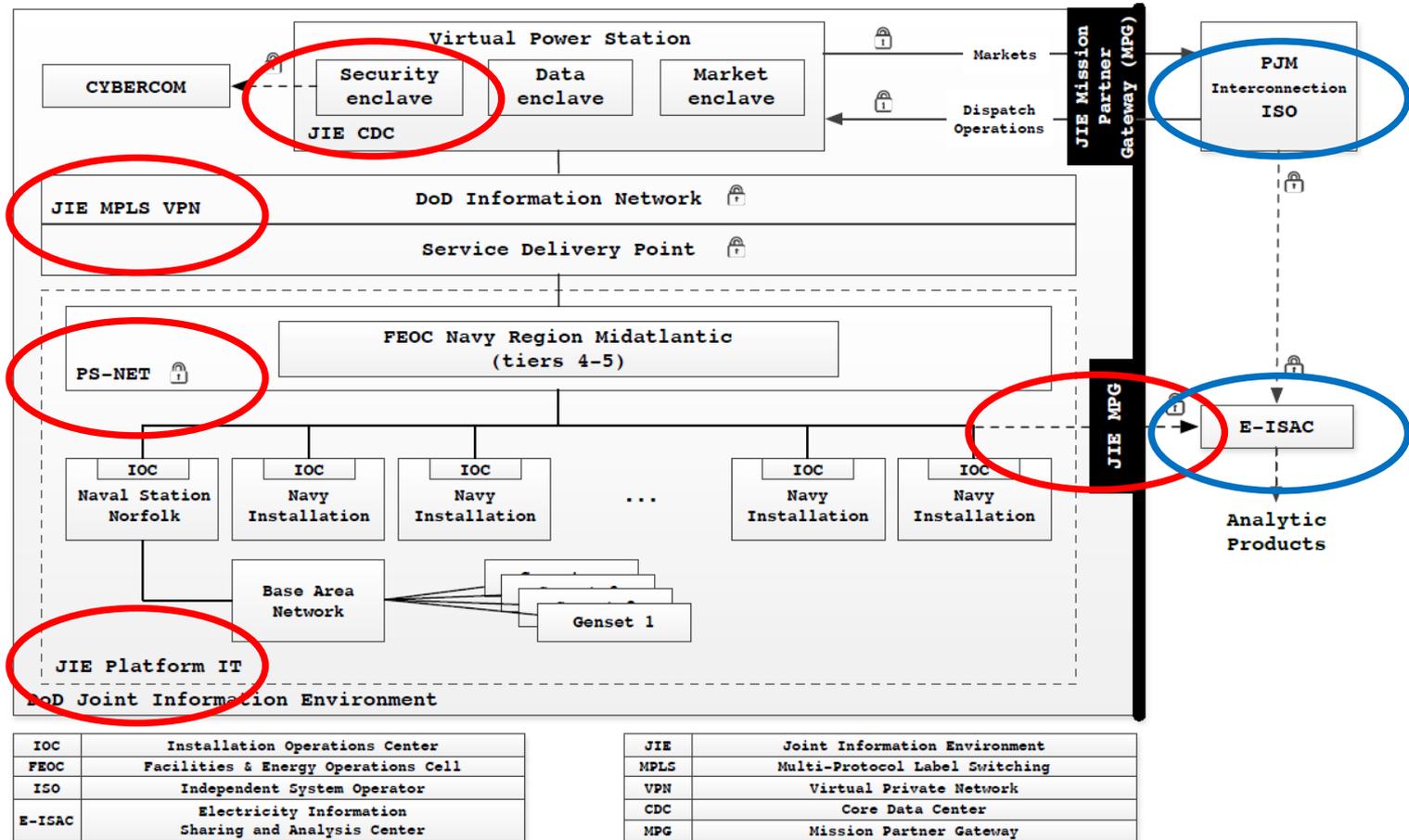
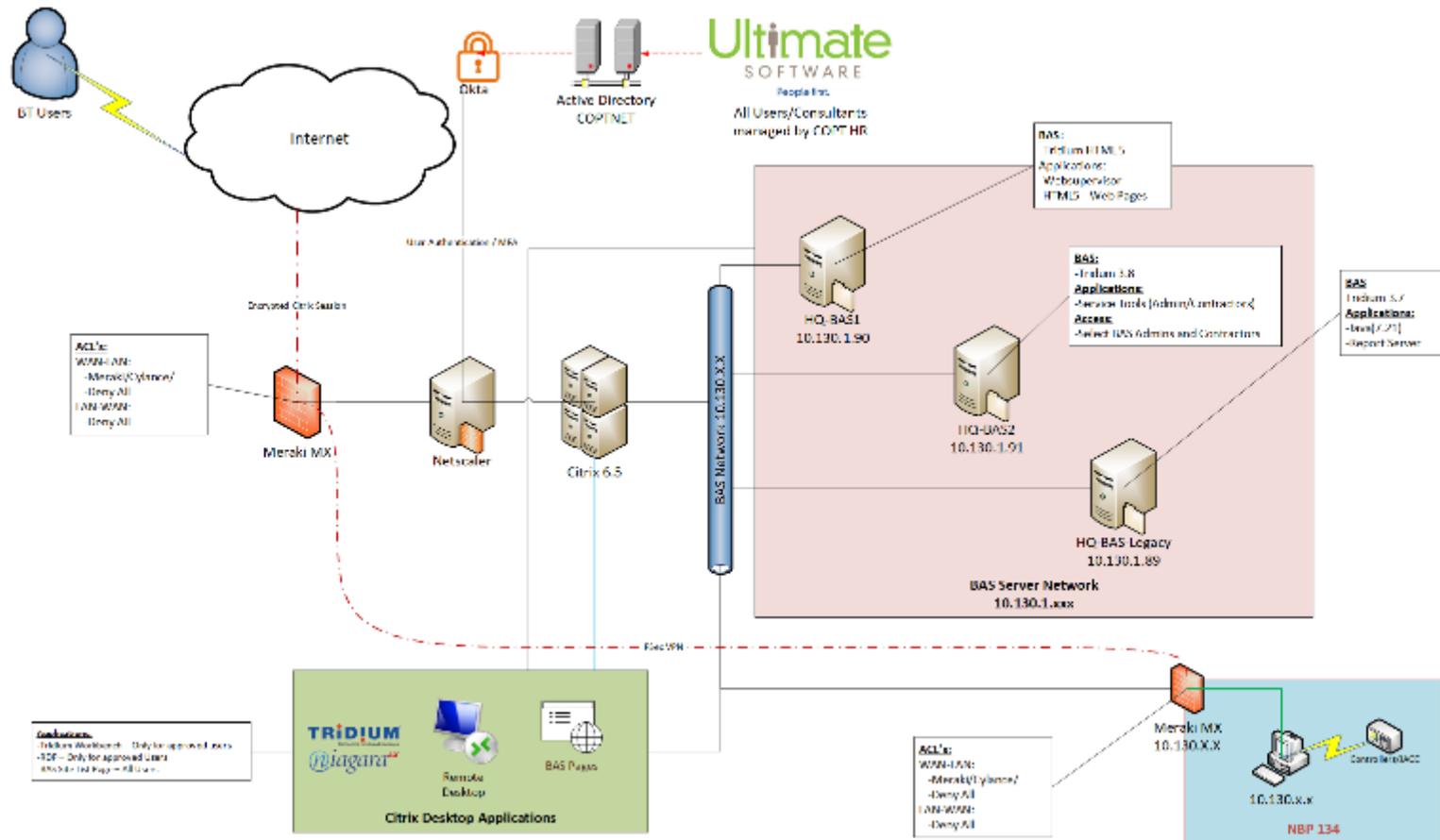


Figure 1. VPS architectural diagram showing network connections and participating entities.

COPT Building System Network and Security Overview



Background

- Scope of discussion – “outside the fence” COPT properties
 - Multi-tenant space
 - May include tenants who support DoD/IC but not exclusive to
- Unclassified networks and data
- No SSP, POA&M, or any other type of certification/accreditation requirement in place with the government or any other tenant for these networks and systems
- Not subject to FAR/DFAR requirements – no existing requirements for the lease of real property
 - No specific cybersecurity related requirements contained in existing lease documents imposed upon COPT
- No existing DoD/IC policy dictating cybersecurity requirements for leased facilities

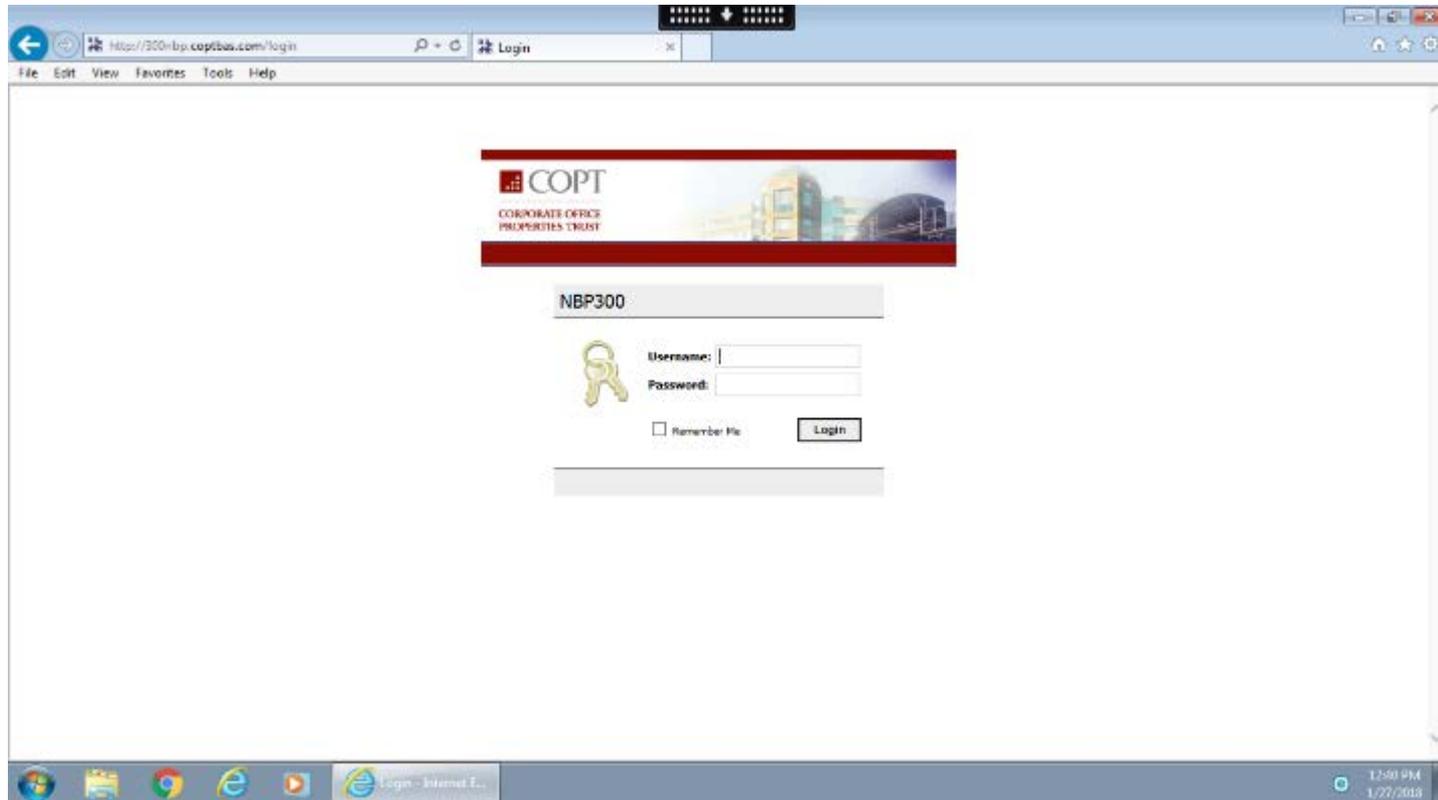
Risk Management

- Started heading this direction in June 2016
- NIST Cybersecurity Framework
 - Two spins (1 internal / 1 external)
 - Established baseline maturity model for COPT cybersecurity posture
- NIST 800-171 – “Protecting Unclassified Information in Non-Federal Information Systems and Organizations”
 - Completed initial assessment (Dec 2017)
 - Scoped to today’s discussion
 - Established a working System Security Plan and Plan of Action & Milestones for identified gaps
 - DFAR 252.204-7012
- NIST 800-82 – “Guide to Industrial Control Systems Security”
 - Out of scope for today’s discussion – Examining for DC-6 and other COPT properties as appropriate

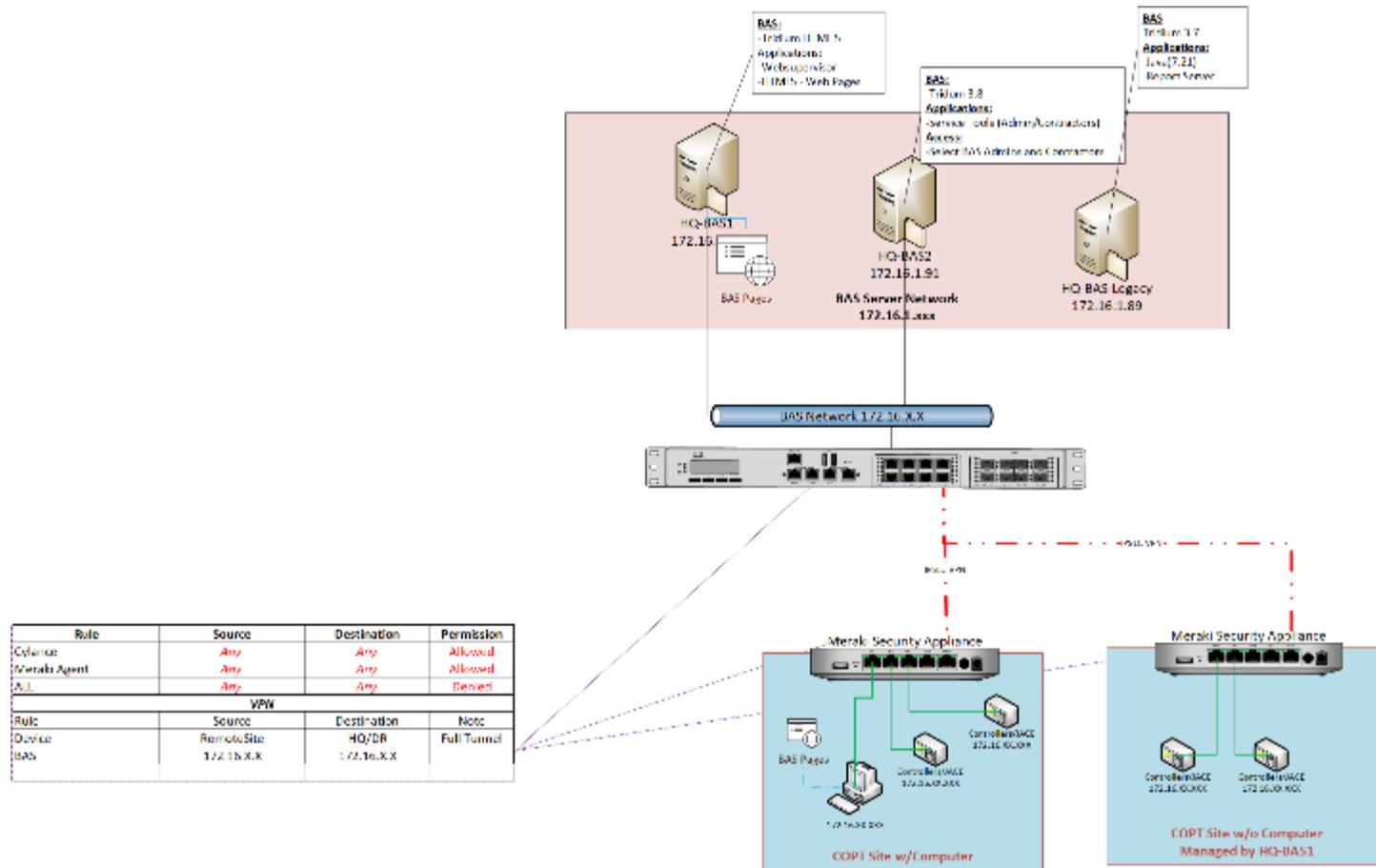
“Interaction with secure spaces”

- It depends on your perspective...(2 of 2)
- The technical answer is no, these systems do not interact with any secure spaces in any of COPT’s “outside the fence” properties
- Access control systems to suites – as a general rule – are the responsibility of the tenant
- HVAC, Lighting, Fire, Common Area Physical Access, Water, etc, are physically isolated systems outside of a tenant’s SCIF boundary
- The “gray area” is why COPT is proactively taking steps to ensure these systems are appropriately protected

User Interface to Building System



COPT Building System – Future State



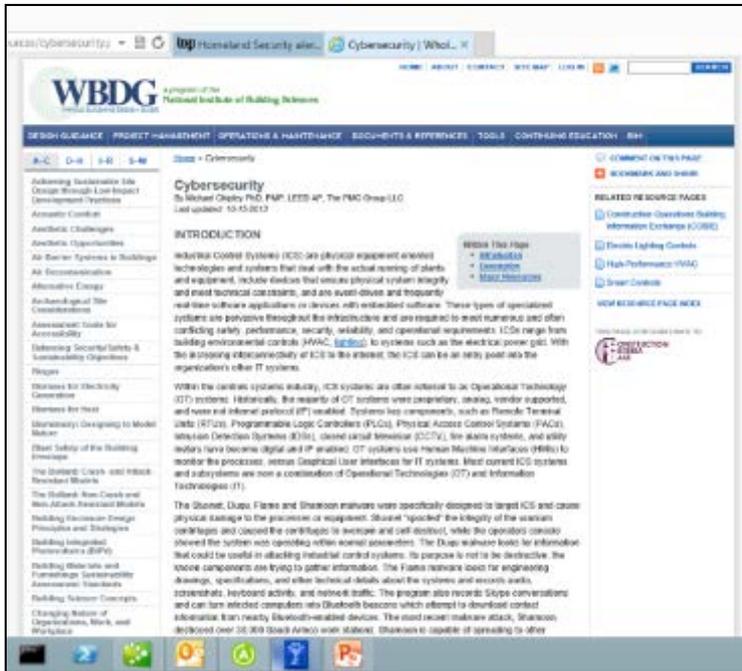
Future Enhancements

- The “80% solution” iterative development/deployment
- Continue converting/cutting over COPT “outside the fence” properties
- Continue modernization of building systems to migrate away from Java dependent enclaves
- “Building system” Active Directory domain
 - 1-way trust from COPT corporate domain
 - Role based access account provisioning/de-provisioning within the building system environment
- Multi-factor for all versions of remote access to all COPT environments
 - Inside and outside the fence
 - Okta app / email doesn’t solve for behind the fence
- Continuous monitoring internal to building network only
 - Multi-tenant environment vice combined
- Change over building system IP space to separate RFC-1918 addressing
- Security awareness training for COPT employees specific to industrial control systems

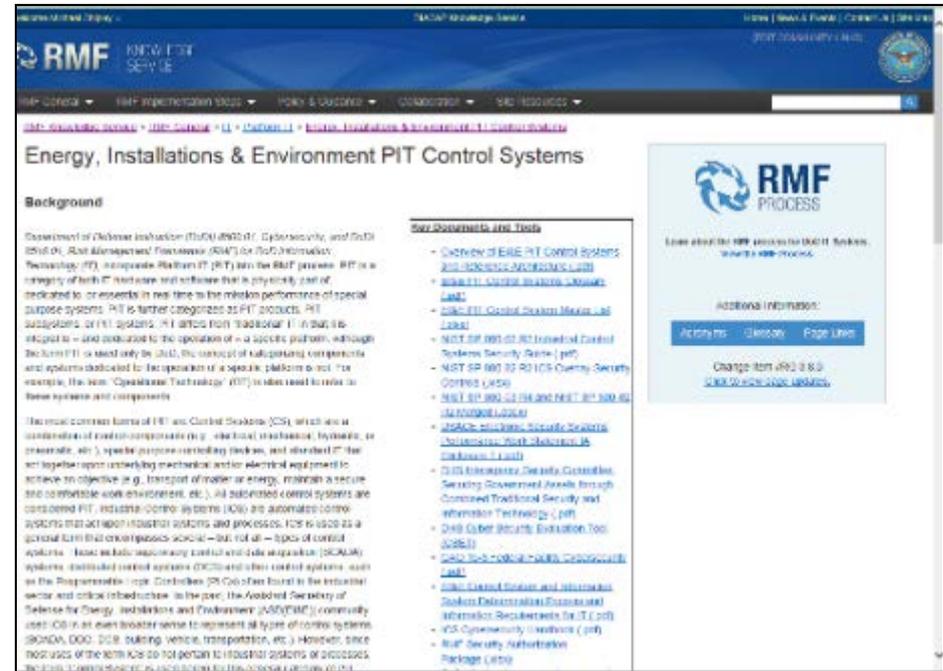
Conclusions

- DoD is moving to Cloud services very quickly
- Understand cloud architectures for FRCS
- FRCS data will generally be Level 4 CUI Moderate Impact
- Virtualization and Visualization offer major cost savings
- Cybersecurity of cloud much better than keeping old architectures and services
- Don't be afraid of the Cloud!

EI&E Cyber Resources



The screenshot shows the WBDG Cybersecurity page. The header includes the WBDG logo and navigation links. The main content area is titled "Cybersecurity" and features an introduction section. The introduction discusses Industrial Control Systems (ICS) and Operational Technology (OT) systems, highlighting their physical nature and the challenges they pose for cybersecurity. It mentions that ICS/OT systems are often overlooked in traditional IT security frameworks and that they have become digital and IP-enabled, increasing their vulnerability to cyber threats. The text also notes that ICS/OT systems are often used in critical infrastructure and that their compromise can have significant consequences.



The screenshot shows the RMF Knowledge Service page. The header includes the RMF logo and navigation links. The main content area is titled "Energy, Installations & Environment PIT Control Systems" and features a background section. The background section discusses the Department of Defense Information (DOD) Cybersecurity and Risk (DOD) Risk Management Framework (RMF) for Risk Information Technology (IT), Information Risk (IT) and the RMF process. It notes that PIT is a category of both IT hardware and software that is physically not dedicated to or essential in real time to the mission performance of special purpose systems. PIT is further categorized as PIT products, PIT subproducts, or PIT systems. It is defined as a specific platform, although the term PIT is used only in DOD, the concept of subplatform components and systems applicable to the operation of a specific platform is not. The term "Operational Technology" (OT) is used to refer to these systems and components. The text also mentions that the most common form of PIT are Control Systems (CS), which are a combination of hardware and software (e.g., electrical, mechanical, hydraulic, or pneumatic), specific process controlling devices, and standard IT that work together to control mechanical and/or electrical equipment to achieve an objective (e.g., transport of water or energy, maintain a secure and controlled work environment, etc.). All supported control systems are considered PIT. Industrial control systems (ICS) are automatic control systems that control industrial systems and processes. ICS is used as a general term that covers process control, but not all types of control systems. Basic safety emergency control and other equipment (ESCAL) systems, distributed control systems (DCS) and other control systems, such as Programmable Logic Controllers (PLC) can often be found in the industrial sector and critical infrastructure. In the past, the Assistant Secretary of Defense for Energy, Installations and Environment (ASD/EIE) community used ICS in an even broader sense to represent all types of control systems (SCADA, DOD, DOD, building, vehicle, transportation, etc.). However, since most users of the term ICS do not pertain to industrial systems or processes, the term "Operational Technology" is used to refer to these systems and components.

<http://www.wbdg.org/resources/cybersecurity.php>

Navigate to DoD CIO Knowledge Service (requires CAC)
<https://rmfks.osd.mil/login.htm>

SERDP & ESTCP Webinar Series

For additional information, please visit
[http://www.wbdg.org/resources/
cybersecurity.php](http://www.wbdg.org/resources/cybersecurity.php)

Speaker Contact Information

mchiple@pmcgroup.biz; 571-232-3890



Q&A Session



The next webinar is on
April 5, 2018

*Advanced Nanocrystalline Cobalt Alloys
and Composites as Alternatives for
Chromium and Nickel Plating in Repair
Operations*



Survey Reminder

Please take a moment to complete the survey that will pop up on your screen when the webinar ends

